REMARKS

Reconsideration and further examination is respectfully requested. Claims 13-17, 37-47 and 67-69 are cancelled by this amendment.

Rejection under 35 U.S.C. §101:

Claims 66-69 were rejected under 35 U.S.C. §101 as directed to non-statutory subject matter. Claims 67 -69 have been canceled.

Rejections under 35 U.S.C. §102

Claims 13-17:

Claims 13-17 were rejected under 35 U.S.C. §102(b) as being anticipated by Mittra, U.S. Patent 5,748,736. Claims 13-17 have been cancelled.

Claims 48-64:

Claims 48-64 were rejected under 35 U.S.C. §102(b) as being anticipated by Gupta (U.S. Patent No. 6,718,387).

Gupta:

Gupta describes, at columns 5-6:

"... FIG. 5 is a diagram of extension to an Internet Group Management Protocol (IGMP) join request in accordance with one aspect of the invention. A header 500, and packet type shown in Field 1 together with a requester IP address shown in Field 2 would typically be part of prior art IGMP join request. In the extensions shown in accordance with one aspect of the invention, an optional timestamp may be placed in Field 1 and a random key, placed in Field 3, is generated by the requester. The contents of Field 1, Field 2 and Field 3 are encrypted or digested and the digest

encrypted and placed into Field 4. The Cyclic Redundancy Check 510 (CRC) encompasses the full IGMP join request..."

Gupta further describes, at column 6, lines 20-44, in part:

FIG. 6 is a flow chart of an exemplary routing element process for determining whether to permit or reject an IGMP join request in accordance with one aspect of the invention. When an extended IGMP join request is received at a router (600) determination is made from the address whether or not the multicast is public or private (605). If it is public (605-public), the join is permitted and the join request forwarded to the next routing element along the path, if any (640). If the multicast is private (605-private) a check is made to determine whether the join request submitted is a duplicate of a previous request. One way an unauthorized user may attempt to gain access to a multicast would be to duplicate a join request submitted by a previous user. If the submitted join request is a duplicate (610-y), the request is rejected. If it is not, a determination is made whether the join request is timely (615). This a simple check to see that the join request is appropriate for the day and time of the current multicast session. This would prevent a user from copying an earlier join request from an authorized user in an attempt to gain access to the current session. If the join request is not timely (615-N), the request to join is rejected. If it is timely, a check is made to determine whether the join request came from a proper link. If it did not (620-N), the join request is rejected. However, if it did, the routing element will obtain the public key dual corresponding to the private key utilized to encrypt the IGMP extended join request (625). Preferably, the public key is obtained from a DNS server, such as DNS 130 shown in FIG. 1. Alternatively, the public key; could be obtained from a certification authority 150 shown in FIG. 1. Using the acquired public key, Field 4 of the extended IGMP join request is decrypted using the public key (630). The resulting information decrypted from Field 4 should agree with Fields 1-3. If it does, the join is permitted and the join request is forwarded to the next routing element. If it does not (635-n), the join request is rejected and the user will be denied access to the multicast by the router.

Thus Gupta describes only the receipt of a join request from a router. In contrast, claim 48 as amended now recites "...receiving, from a designated routing device coupled to a host, an encoded join request for a the host device, the encoded join request being encoded by the designated routing device using an authentication key associated with the host ... authenticating the encoded join request to determine whether or not the encoded join request is authentic; and establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be

authentic..." In the system of Gupta, there is no mention or suggestion of the join request being encoded by the designated router. Rather, the join request comes directly from the host. For at least this reason, it is submitted that claim 48 is patentably distinct over Gupta, and the rejection should be withdrawn.

Independent claims 53 and 58 are apparatus and computer program claims which have been amended similar to claim 48, and are allowable for reasons similar to those discussed with regard to claim 48. For example, both claims 53 and 58 have been amended to include the limitation of "...receiving logic programmed to receive an encoded join request for a host device receiving logic operably coupled to receive an encoded join request for a host device, the encoded join request being encoded and forwarded by a designated routing device coupled to the host device ..." Accordingly, for at least the reason that Gupta fails to describe or suggest every limitation in the claim, it is respectfully submitted that the rejection has been overcome and should be withdrawn.

Dependent claims 49-52, 54-57 and 59-64 serve to add further patentable limitations to their parent independent claims, but are allowable for at least the reasons put forth with regard to those claims.

Claims 66 & 67:

Claim 66 is rejected under 35 U.S.C. §102(b) as being anticipated by Ballardie. Claim 67 was rejected under 35 U.S.C. §102(b) as being anticipated by Fan (U.S. Patent No. 6,664,922). Claim 67 has been cancelled.

Claim 66, as amended, now recites "...A communication message embodied in a data signal which is forwarded between computer devices in a computer network, the communication

message comprising a group key for a multicast group and an authentication key for use in authenticating multicast membership requests by a host device...."

Although Ballardie describes, at page 11, that 'The host key pair is encrypted using the public key of the originating host, so as to be only decipherable by the originating host...' it neither describes nor suggests a communication message comprising *both* a group key and an authentication key to be used for authenticating multicast membership requests by the host device. Rather, Ballardie only describes that the key associated with the originating host is used to encode the communications. Accordingly, for at least the reason claim 66 is patentably distinct over Ballardie.

Rejections under 35 U.S.C. §103

Claims 1-4, 7-12 and 65:

Claims 1-4, 7-12 and 65 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra (U.S. Patent 5,748,738) in view of Gupta and further in view of Ballardie.

Mittra:

Mittra describes a system and method for secure group communication via multicast or broadcast transmission. In preferred embodiments, the system of the invention implements a secure multicast group consisting of senders, receivers, a group security controller (GSC), and at least one trusted intermediary (TI) server. The GSC and each TI server are responsible for maintaining the security of the group by authenticating and authorizing all other members of the multicast as well as managing the group key(s) (Kgrp(s)) that are used to encrypt the messages

multicast to the group. (Mittra, Abstract). With regard to the joining and leaving of a group, Mittra describes, at column 13, lines 37-50:

> "... From the joining member's vantage, joining a secure multicast group is identical to the procedure described above (without reference to trusted intermediaries) except that the member either contacts its parent TI server or the GSC depending on its access point in the hierarchy of the group. If the access point is at a level such that the joining member contacts not the GSC but a parent TI server (e.g., in the case that receiver 114f of FIG. 1 seeks to join the group consisting of all elements of FIG. 1 other than receiver 114f, in which case receiver 114f would contact TI server 115c rather than GSC 111), the TI server performs authentication on behalf of the GSC and changes the Kgrp (for its sub-group) using the above-described procedure performed by the GSC (to perform authentication and change the Kgrp). ..."

Thus Mittra describes a system wherein authentication of a host is performed by the 'closest' trusted router (i.e., the trusted intermediary). Gupta, as described above, describes a system whereby a host authenticates through direct contact with the GCKS. Thus in essence both system describe a situation wherein authentication is performed between a host device and the nearest trusted device. Such a structure neither describes nor suggests the claimed structure of the present invention, wherein the elements of the claim perform the claimed functions.

For example, claim 1 recites "...A communication system comprising: a rendezvous point device... a designated device in communication with the rendezvous point device ... and a host device in communication with the designated device, wherein: the host device sends a join request to the designated device using a predetermined multicast group management protocol in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device; *the designated device receives the join request and forwards to the rendezvous point device via the number of intermediate devices an encoded join request generated using an authentication key associated with the host device...*"

The Examiner states at page 6 of the Office action:

"Mittra discloses a communication system comprising ... a rendezvous point device ... a designated device in communication with the rendezvous point device (see col. 12, lines 50-59)... a host device in communication with the designated device ... Mittra does not explicitly disclose but Gupta discloses the host device sends an encoded join request generated using an authentication key associated with the host device using a predetermined multicast group management protocol..."

Applicants would like to bring the Examiner's attention to the language of the claims, as it appears that there is some confusion. The claim language does not state that the encoded join message is forwarded by the host, but rather that "...the **designated device** receives the join request and forwards ... an encoded join request generated using an authentication key associated with the host device..." Such a structure is neither shown nor suggested by the combination of references put forth by the Examiner. In addition, several other limitations are not shown or suggested by the combination of references put forth by the Examiner.

For example, if the Examiner characterizes the trusted intermediary device of Mittra as the 'designated router' of the claimed invention, it is clearly stated in Mittra that 'the TI server performs authentication on behalf of the GSC', and thus authorizes join requests itself, without forwarding to the GSC. Accordingly, the combination of references would therefore neither describe nor suggest the forwarding of the join message from the host to the rendezvous point.

The Examiner states that 'it would have been obvious to one or ordinary skill in the art at the time the invention was made to implement the teaching of Mittra's secure group communication via multicast with the teaching of Gupta's encoded join request in order to prevent unauthorized users from gaining access to a multicast by duplicating other's join request..." However, Applicant's maintain that even if a motivation could be found to encode

the join request, the encoding would be performed by the host, rather than an intermediary device.

The Examiner further states that 'Mittra does not explicitly disclose but Ballardie discloses the designated device receives the join request and forwards to the primary core of a basic tree (CBT) via the number of intermediate devices ... Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Mittra's secure group communications via multicast with Ballardie's teaching of forwarding the join request from the secondary device to the primary device via a number of intermediary devices so that the host can send the join request to its local multicast router..."

Applicants disagree that a motivation for the modification suggested by the Examiner can be found in the references. Mittra explicitly states, at column 12 'TI servers are authorized to act as proxies for the GSC. Each TI server can approve changes in group membership below it...thus isolating the effects of these changes in group membership..." Applicant's submit that the teaching of Mittra teaches directly away from the modification suggested by the Examiner, of 'forwarding the join request from the secondary device to the primary device...'.

Accordingly for at least the reasons stated above, and also because the combination of references neither describes nor suggests the limitations of the claims, claim 1 is patentably distinct over the combination of references, and the rejection should be withdrawn.

Claims 2-12 serve to add further patentable limitations to claim 1 but are allowable for at least the reason that they depend upon an allowable parent claim.

Claim 65 recites "... In a communication system having a host device, a designated device, and a rendezvous point device, a method comprising ... sending a join request by the host device to the designated device in order to join a shared tree ... sending an encoded join

request by the designated device to the rendezvous point device ... authenticating the encoded join request by the rendezvous point device ... adding the host device to the shared tree, if the encoded join request is authentic ... and excluding the host device from the shared tree, if the encoded join request is not authentic..." Thus claim 65 recites structure similar to that described above with regard to claim 1, and is therefore allowable for reasons similar to those put forth with regard to claim 1.

Claims 5 and 6:

Claims 5 and 6 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra in view of Gupta and Ballardie as applied to claim 4, and further in view of Fran (U.S. Patent 6,664,922).

Fan describes, in the Abstract, a method for distributing locating-relevant information includes providing a GPS position of a client to a server on a data network, and returning location-relevant information by the server based on the specified GPS position. At column 9, Fan states that "...The data processing program can also receive a request from monitor unit 22. Typically, such a request is provided with an authentication key over data network 27..." (column 9). Fan's 'request' is generally a request for directions, and thus not analogous to a multicast membership request. In addition, even if it could be argued that the authentication key of Fan could be used with a multicast membership request, the addition of Fan to Mittra, Ballerdie and Gupta still fails to overcome the inadequacies of the combination of references as recited above. Accordingly, for at least this reason, claims 5 and 6 are patentably distinct over the combination of references, and the rejection should be withdrawn.

Claims 18-19 and 20-25:

Claims 18-19 and 20-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gupta in view of Fan.

Claim 18, as amended, now recites "...An apparatus comprising...receiving logic operably coupled to receive an authentication key; and joining logic operably coupled to send a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key *to enable the designated device to encode the join message for authentication by a rendezvous point...*" No such structure is shown or suggested in the combination of Gupta and Fan. Accordingly, for at least this reason, the rejection is overcome and should be withdrawn.

Independent claims 20 and 22 have been amended to include limitations similar to those of claim 18, and are therefore allowable because the combination of references neither describes nor suggest the elements of the claims. Dependent claims 19, 21 and 23-25 depend on claims 18, 20 and 22, respectively, serve to add further patentable limitations to their parent claims and are allowable for at least the same reasons as their parent claims.

Claims 26, 29, 32, 37, 40, 43 and 46-47

Claims 26, 29, 32, 37, 40, 43 and 46-47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra (U.S. Patent No. 5,748,736) in view of Gupta (U.S. patent No. 6,718,387). Claims 37, 40, 43 and 46-47 have been canceled.

Mittra and Gupta have been described in detail above. Applicant's claim 26 recites "...A method comprising receiving a join request from a host device ... generating an encoded join request using an authentication key associated with the host device; and sending the encoded join

request toward a rendezvous point device..." Applicant's claim 29 recites "...An apparatus comprising... receiving logic operably coupled to receive a join request from a host device; encoding logic operably coupled to generate an encoded join request using an authentication key associated with the host device; and sending logic operably coupled to send the encoded join request toward a rendezvous point device..." Applicant's claim 32 is directed to a computer program, but includes similar limitations to claims 26 and 29.

As described above with regard to claim 1, no mention or suggestion is found in the combination of references of a method wherein encoding of a join request is performed at an intermediary point in a transmission sequence. Accordingly, for at least this reason, claims 26, 29 and 32 are patentably distinct over the references and the rejection should be withdrawn.

Claims 27, 30 and 33

Claims 27, 30 and 33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra in view of Gupta and further in view of Fan.

As described above with regard to claims 26, 29 and 32, the combination of Mittra and Gupta neither discloses nor suggests a structure such as that in the recited claims. Fan, which is drawn to a GPS direction system, does nothing to assist in overcoming the deficiencies of Mittra and Gupta with regard to the independent claims. Accordingly, for at least the reasons that claims 26, 29 and 32 are patentable, claims 27, 30 and 33 are also patentable over the combination of references, and the rejection should be withdrawn.

Claims 28, 31 and 34, 38-39, 41-42 and 44-45

Claims 28, 31 and 34 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra in view of Gupta and further in view of Ballerdie. Claims 38-39, 41-42 and 44-45 have been canceled.

As described above with regard to claims 26, 29 and 32, the combination of Mittra and Gupta neither discloses nor suggests a structure such as that in the recited claims. Ballerdie does nothing to assist in overcoming the deficiencies of Mittra and Gupta with regard to the independent claims. Accordingly, for at least the reasons that claims 26, 29 and 32 are patentable, claims 28, 31 and 34 are also patentable over the combination of references, and the rejection should be withdrawn.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone the undersigned, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

10/28/2004
Date

Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-244
Dd: (original) 10/28/2004